

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

RECEIVED

JUN - 5 1997

In the Matter of

Federal Communications Commission
Office of Secretary

Electronic Filing of Documents in
Rulemaking Proceedings

GC Docket No. 97-113

DOCKET FILE COPY ORIGINAL

REPLY COMMENTS OF GTE SERVICE CORPORATION

GTE Service Corporation on behalf of its telephone and wireless subsidiaries ("GTE") hereby submits its reply comments in response to the *Notice of Proposed Rulemaking* ("NPRM") adopted by the Federal Communications Commission ("FCC" or "Commission") in the above-captioned proceeding.¹ In the *NPRM*, the Commission proposes to allow parties to file comments and other pleadings electronically in notice and comment rulemaking proceedings, except for broadcast allotment proceedings. As noted herein, GTE supports the Commission's efforts to phase in electronic filing. Comments filed in response to the *NPRM* unanimously supported adopting an electronic filing capability. Chief among the concerns of interested parties, however, was development of some method of ensuring the security of Internet transmissions.

I. Discussion

GTE and all other commenters in this proceeding were unanimous in their support for electronic filing. These comments provide the FCC with a clear mandate to quickly adopt the rule changes needed to give pleadings filed electronically the same formal status as pleadings currently filed on paper.

¹ Electronic Filing of Documents in Rulemaking Proceedings, *Notice of Proposed Rulemaking*, GC Docket No. 97-113, FCC 97-113 (released April 7, 1997).

In adopting an electronic filing capability, there are a number of issues the FCC must work through. Thus, as GTE indicated in its comments, the FCC must consider measures to ensure that parties are able to send electronic transmissions in the afternoon on days when comments in many popular proceedings are due; how the official filing time will be determined; how to deal with page counts and citation to documents filed electronically; and how to ensure that copies of electronically filed documents are made available to public.

The issue that received the most attention by commenters, however, was the issue of security of transmissions. The FCC stated in the NPRM that it did not believe the risk of forgery of electronically filed documents is any greater than the risk with paper filed documents.² GTE generally agreed with that statement, but pointed out that the risk of transmission error present in filing documents electronically justifies an examination of methods of ensuring accurate and secure transmissions. GTE stated in its comments that the FCC's electronic filing system platform should enable parties that wish to use and pay for measures that better guarantee the accurate transmission of data are able take such measures. GTE stated it believed such a capability could be implemented at very little cost to the Commission.³

Numerous other parties raised security issues associated with filing comments on the Internet. AT&T, for example, recommended that the Commission "permit parties that expect routinely to participate in future rulemaking proceedings to apply for a

² NPRM at 6-7 (¶ 16).

³ GTE Comments at 5-6.

password that they can use to identify their electronic filings."⁴ NECA and PCIA recommended that the Commission assign account numbers that must be entered when transmitting comments.⁵ Bell Atlantic and NYNEX suggested that the Commission "examine various forms of Web-based electronic signature or digital certificates that are currently under development."⁶ On the other hand, U S WEST and Cincinnati Bell stated that they do not believe special security measures are required.⁷

GTE believes that the FCC can implement a system that satisfies each of these parties' concerns. Thus, GTE recommends that the Commission put in place the ability for parties to voluntarily use digital identification measures or "digital certificates" to ensure secure delivery of the their pleadings.⁸ GTE has attached as Appendix A a white paper written by GTE Government Systems Corporation, that discusses both the need for secure Internet transmissions and various means, including digital certificates, of assuring that transactions between two parties on the World Wide Web are safe and secure.

While digital certificates owe their origin to the security concerns surrounding financial transactions on the Internet, their key features will address a number of issues involved in the electronic filing of pleadings with the FCC. Digital certificates allow

⁴ AT&T Comments at 5. See *also* Ohio Consumers' Counsel Comments at 4, SBC Comments at 6.

⁵ NECA Comments at 4; PCIA Comments at 3.

⁶ Bell Atlantic and NYNEX Comments at 4.

⁷ US West Comments at 4; Cincinnati Bell Comments at 5.

⁸ Such a system can work instead of or in addition to a system that uses passwords or account numbers.

parties to elevate their communications to a level of security that: (i) authenticates the identity of both parties involved; (ii) protects the integrity of the data such that any changes made to it (either accidentally or maliciously) will be quickly identified; and (iii) provides proof that both parties participated in the communication should one party subsequently deny involvement. A technical discussion of how digital certificates accomplish this through means of encryption can also be found on GTE's CyberTrust homepage at <http://www.cybertrust.gte.com>.

GTE urges the Commission to consider including digital certificates in the initial design of the electronic filing system. GTE believes that the electronic filing system can be designed such that the use of digital certificates would be entirely up to the filing party. By not requiring parties to use digital certificates, any party that does not have concerns over security would not be forced to take steps necessary to use them or incur any costs associated with them.⁹ Parties that choose to use digital certificates would bear the costs associated with their use.¹⁰ GTE would be happy to meet with the

⁹ Eliminating the need to obtain FCC passwords to file electronically may cause more parties to file electronically. One-time or infrequent commenters may find the process of applying for a FCC password burdensome and thereby not request one, thus preventing them from filing their comments electronically.

¹⁰ There are basically two Web-based forms of digital certificates. The certificate that installs in a Internet Web browser (e.g., Netscape or Microsoft Explorer) is called an end user certificate. The certificate that installs on the Web-based server is called a server certificate. Server certificates can currently be purchased for under \$500 and end user certificates for under \$20. To implement the capabilities GTE suggests, the FCC would need to install a server certificate, while each party wishing to secure transmissions to the FCC would need to install an end user certificate. The price of end user or server certificates should not present a financial barrier for inclusion in the Commission's electronic filing system.

Commission should FCC staff want more information about electronic security measures.

II. Conclusion

GTE supports the Commission's efforts to phase in electronic filing. GTE believes that the Commission should consider implementing in its electronic filing system, measures that will enable a party to ensure the secure transmission of information to the Commission if the party elects to do so. Thus, GTE recommends that the Commission put in place the ability for parties to voluntarily use digital identification measures or "digital certificates" to ensure secure delivery of the their pleadings.

Respectfully submitted,

GTE Service Corporation and its telephone
and wireless companies

By Andre J. Lachance

Andre J. Lachance
1850 M Street, N.W.
Suite 1200
Washington, DC 20036
(202) 463-5276

June 5, 1997

Their Attorney

ATTACHMENT A

Digital Identification the Passport to Secure Electronic Commerce

"We stand on the edge of a coming explosion in Internet economic activity."¹



White Paper
March 1997

© 1997 GTE Government Systems Corporation.

Digital Identification the Passport to Secure Electronic Commerce

The New Internet Marketplace

Electronic commerce – the transaction of business over the Internet – has been likened to the Gold Rush, with its great promise of hidden riches. Forrester Research predicts that by the year 2000, the Internet economy will top \$200 billion in the U.S. alone. Beyond the financial incentives, the Internet also promises to overhaul the way business is conducted, creating more flexible business processes, greater business-to-business intimacy and tighter relationships with consumers.

Within today's consumer market, customers are turning to the Web primarily to browse, not to buy. Instead, they typically log off and call a toll-free number to place an order and pay. We are still a long way from achieving the full potential of electronic commerce, which encompasses a comprehensive array of Web-based offerings from home banking and shopping to premium information services.

Among businesses, the Internet offers a fast and cost-effective means of interacting with suppliers, partners and customers. Whether linking vendors up and down the supply chain, conveying confidential information within the corporate hierarchy or delivering information about products and services, the Internet enables tighter business relationships than ever before. Yet, many businesses have been hesitant to incorporate electronic commerce into their operations, in spite of these benefits.

To achieve its full potential, electronic commerce must deliver the same levels of privacy, integrity and trust that traditional business practices enjoy. Market research by O'Reilly & Associates suggests that security concerns are a major obstacle to doing business over the Internet. But less than one percent of today's commercial sites on the World Wide Web are

equipped to deliver secure transactions according to O'Reilly.

The Internet is unquestionably the marketplace for the new economy. But before online transactions can become as commonplace as face-to-face banking or credit card encounters, the technology must be in place to protect buyers and sellers from hackers and unscrupulous merchants.

The future of Web-based commerce depends to a large extent on the question: Will the Internet ever be secure?

"1997 will be the year when Web merchants rethink their strategies in light of growing consumer concerns about security. It may also be the year when semiorganized hackers and virus creators will infect 20 to 30 percent of web sites. That will cause buyers to have second thoughts about dealing with online merchants."²

Vic Wheatman, analyst, Gartner Group

Internet Security

When it comes to business, the Internet must be as safe and secure as a face-to-face exchange. But the old standards of trust, beginning with eye contact and a firm handshake, are not possible when business and legal transactions are moved onto the World Wide Web.

To do real business online – everything from paying a bill and transferring funds to buying stocks – there must be an infrastructure in place to mirror the time-honored ethics of trust. This infrastructure must provide the means to verify the identity of each participant in a binding transaction.

The following issues must be addressed in creating the infrastructure to support electronic commerce:

- *Privacy.* In a network-based transaction, there must be reasonable assurances that any information exchanged remains private between the sender and the receiver.
- *Authentication.* On the Internet, everyone is anonymous. In order to engage in a business transaction, each party must be able to authenticate the other's identity.
- *Integrity.* Once a party signs a transaction, it must be protected from tampering or forgery. The integrity of a transaction is particularly important in sales where prices, terms and quantities are agreed upon as part of the deal.
- *Nonrepudiation.* After a transaction has been made, it cannot be revoked. Neither party involved in the transaction can deny their role in the exchange. This provision makes it impossible for either party to make false claims about the offer made or accepted.
- *Support of the legal system.* Electronic commerce must be recognized and supported by the legal system. A digital signature on a document must carry the same weight in a court of law as a written signature.

In virtually every industry, the everyday exchange of goods, funds or documents involves a corresponding exposure of private, confidential information and any security breach could have

serious consequences. What if a soft drink company placed an electronic order for ingredients that exposed the secret formula for a new beverage? Such opportunities for malicious intervention must be averted.

Or consider another example: An investor wants to buy 1,000 shares of a stock at \$20 a share. There must be a way of authenticating the identity of the investor, confirming the integrity of the terms, verifying the shares of stock being purchased and assuring that the deal has not been altered. Neither party can be able to tamper with or deny their role in the transaction.

Credit card security a significant concern for businesses and consumers alike. Consumers must have confidence that their private credit card information is safe as it passes over the public Internet and that it is being received by a legitimate business. Likewise, businesses must be confident that they are receiving accurate order information from legitimate cardholders. Otherwise, both parties are exposed to the risk of fraud.

"Consumer confidence is commonly identified as a major stumbling block to selling via the Web. Our results suggest that huge opportunities still exist in this new channel, both for businesses addressing their customers' concerns by offering secure transactions and for companies supplying the technology to help businesses sell online."³

Dick Peck, vice president of business development at O'Reilly & Associates

"The technology to support an electronic commerce infrastructure exists. To make electronic commerce a reality, a critical mass of businesses and consumers must begin to participate in the new methods of establishing trust. This will require not only commitment, but also new tools to help developers easily incorporate the technology into real-world applications."

John Moreh, senior product manager for security with Open Horizon Inc. and a professor at the Department of Engineering and Information System at UCLA

Delivering Digital Security

Imagine you are a store owner. Would you accept a check without identification from a stranger? Think about a vendor placing a multi-million-dollar order using a purchase order that does not belong to his or her company. That's the danger of doing business over the World Wide Web.

To create an infrastructure that addresses the security needs of electronic commerce, leading developers have turned to cryptography, the science of transforming information through encoding and decoding. Although cryptography has been used to protect information for hundreds of years, the speed and power of computers make it possible to use highly sophisticated, secure coding systems that can be quickly applied and removed. This process, known as encryption, delivers the privacy demanded by electronic commerce.

Cryptography also provides a means of bringing authentication, integrity and nonrepudiation to an electronic transaction. A form of cryptography, known as public key technology, can be used to create a system in which consumers, merchants and financial institutions can verify the identity of their counterparts in an

electronic transaction while protecting the information exchanged. This system uses digital certificates to perform this identification [see "How It Works"].

When a consumer writes a check in a department store, he or she is usually required to show some form of identification, such as a driver's license or passport. A credit card fulfills many of the same functions; issued by a trusted third party such as a bank, it identifies the bearer and provides supporting information in the form of an account number, expiration date, signature and sometimes a photo ID.

In simple terms, a digital certificate can be the electronic equivalent of a driver's license, credit card or passport. Digital certificates are issued by a trusted third party, known as a Certification Authority, that verifies the identity of the certificate holder. A digital certificate typically includes identifying information about its holder (e.g., name, address, affiliation), a validity period, a unique serial number and identifying information about the Certification Authority.

Besides authentication, digital certificates can be used to ensure the integrity of an electronic transaction. A digital certificate is issued in conjunction with a particular pair of encryption keys. The private encryption key is used to create a digital signature – a unique encoding of the electronic message – that can only be decoded with the corresponding public key. If the message is altered in any way after it is signed, the recipient will know.

Finally, digital certificates bring a means of nonrepudiation to electronic commerce. They enable the parties in a transaction to positively identify each other and to confirm that the information sent by each party has not been altered en route.

Because of the due diligence performed by the Certification Authority before issuance, digital certificates validate the identity of the businesses, vendors, suppliers and customers involved in an online transaction. The strength of the cryptography ensures the safety of the information exchanged. By resolving these security issues, digital certificates are opening the way for electronic commerce to achieve its full potential.

"In 1997, consumers will start living up to their name on the Internet. People will have digital Ids as forgery-proof as fingerprints. Companies, too, are getting wired, making the Web the business-to-business bazaar of choice."⁵

David Stipp, Fortune Magazine

Beyond Passwords

Consumers and Web merchants aren't the only ones that need digital security. Mainstream businesses of all sizes are concerned about external and internal security as they move their operations online. Companies seeking the benefits of opening their internal networks to the outside world must protect vulnerable corporate information. Whether protecting an order form, sensitive design plans or corporate records, security must be a top priority for any firm considering Internet-based communications.

The threats come from multiple sources, including "spoofing" – the creation of false Web sites that mimic legitimate sites to collect information. Other dangers are the copying and altering of intercepted electronic messages and the illegal invasion of private corporate databases.

To meet these challenges, the information security market is exploding with new technologies that tackle the dual challenge of allowing access to information while, at the same time, protecting that information. Electronic firewalls were initially developed to protect corporate networks from external attack. But as the number of remote users has increased, including telecommuting workers, online business partners and potential customers and suppliers, the demand arose for products that go beyond firewalls to provide privileged information access.

While passwords can be used to provide the access control sought by network managers, they don't always provide the level of security needed. Simple passwords are too easily broken by determined sleuths and present an inconvenience for users who may be asked to remember dozens of alpha-numeric combinations for different accounts.

Digital certificates overcome both the security and convenience limitations of passwords. In simple terms, a digital certificate can function much like a corporate identification badge. Just as a physical badge can be used to determine the parts of a building to which an employee or business partner has access, a digital certificate can be used to control which databases can be viewed. Overall security is improved because outsiders without a badge or certificate cannot gain access to the building or network. And because access privileges are based on information contained in a certificate, the need for passwords is eliminated.

From replacing the password for an online chat room to providing highly restricted access to sensitive corporate data, digital certificate management systems deliver a full range of information access options that can be used to determine who participates in secure electronic commerce.

"Any of the security problems people would have online would be similar to what might happen if you use a charge card in a store. We've seen a lot of hype about Internet fraud, and Hollywood has done movies about it, but the risk is minimized when you transact with merchants over Web sites that work with security compliant software."⁶

Greg Tarmin, senior manager of public affairs for American Express

Embracing Digital Security

With privacy, authentication, integrity and secure access control, the possibilities for electronic commerce are limitless. As consumers gain confidence that their credit card information is safe, the Internet will blossom as the fourth channel of commerce. But the possibilities only begin there.

Companies of all sizes will embrace secure electronic transactions to change the way business is conducted. From collaborative design to just-in-time manufacturing to accounts receivable/payable, companies will be able to communicate internally and externally with much greater confidence that any information exchanged online is secure.

With the movement to more and more business transactions over the Internet, the sweep of digital security will be felt in the far-ranging industries of finance, manufacturing, health care, education and the government. The applications are as varied as the businesses. They include safeguarding electronic funds transfers and securities transactions, preserving the confidentiality of medical records, exchanging confidential information both internally and between vendors and suppliers, protecting classified government agency information, conveying student records and much more. Virtually anything that can be done face-to-face will now be possible online.

The Future of Electronic Commerce is Now

Developments in public key cryptography and certification services will open the floodgates of Internet commerce, and many companies are positioning themselves for the first bursting wave. Microsoft and Netscape have incorporated support for digital certificates into their Web browser and server products.

Likewise, MasterCard, Visa and American Express have joined forces with leading technology developers, including GTE, IBM, Microsoft and Netscape, to formulate the Secure Electronic Transactions (SET) protocol. The SET standard provides a universally accepted means of ensuring the safety of electronic credit card payments.

GTE has subsequently teamed with Wells Fargo Bank to issue the first operational digital certificates to comply with the SET protocol to protect credit card information sent by Web merchants over the Internet.

Providing privacy, authentication, integrity and nonrepudiation over the Internet is becoming a reality. The protection offered by encryption, combined with the positive identification of digital certificates, will virtually remove the security hazards precluding safe business travel on the information highway. With the roadblocks removed, companies can now focus on offering their online customers the trust and integrity traditionally associated with face-to-face transactions.

"A cadre of technology vendors and financial institutions is set to jolt Internet commerce to life with applications and systems based on the SET specification."⁷

Michael Moeller, senior editor, and Jim Kerstetter, staff reporter, for PC Week

The Internet Economy

The Internet Marketplace poses many challenges. But it offers substantial benefits. It can revolutionize the relationships among suppliers, producers and consumers through highly tailored services, enhanced flexibility and even the handing down of corporate cost savings. The Internet can forge new levels of customer intimacy and interactivity for greater one-to-one relationships. In an increasingly hectic world, if the bottom line is convenience, customers will buy.

For the online provider, the ubiquitous and cost-effective Internet and corporate intranet offers quick and easy communication to the outside world. With the infrastructure in place to conduct business securely on the Internet, the momentum of electronic commerce in today's business arena will continue to grow.

How It Works

Public Key Encryption, Digital Signatures and Digital Certificates

To overcome the security problems associated with “blind” electronic transactions, experts have turned to encryption and digital certificates. While the steps to implement the technology are transparent to the user, to understand how it works, we must begin with a brief explanation of public key cryptography.

Cryptography provides the means to protect information by using a mathematical function, or algorithm, to encrypt and decrypt messages. A simple algorithm might replace each character of plain text by skipping two letters, so that A becomes C, B becomes E, Y becomes B and so on.

Encryption algorithms are generally divided into two types: symmetric algorithms and public key algorithms. Conventional algorithms are symmetrical and use the same key for encryption and decryption. Public key algorithms are asymmetrical, requiring the use of two related keys, one for encryption and the other for decryption.

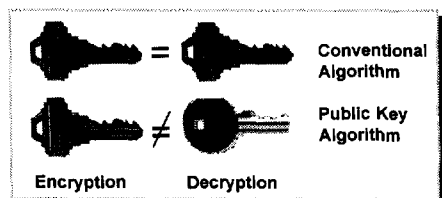


Figure 1. Public key encryption relies on two different, but mathematically related digital keys. It is therefore more secure than conventional, single-key encryption algorithms.

Encryption. In a public key encryption system, information encrypted with a particular public key can only be decrypted with its corresponding private key. Private keys are intended for personal use and need to be securely stored on a computer or a hardware token, such as a smart card. Public keys can be shared either by making them available on an Internet key server or by sending them to partners during the transaction.

Consumers and businesses can use public key encryption to protect the privacy of the information exchanged in an electronic transaction. To protect an order made from a Web site, a consumer can use a copy of the merchant's public key to encrypt the order. When the merchant receives the order, the information can then be decrypted using the corresponding private key. And, as long as the merchant keeps its private key secure, the encrypted order information will be safe and cannot be easily decrypted.

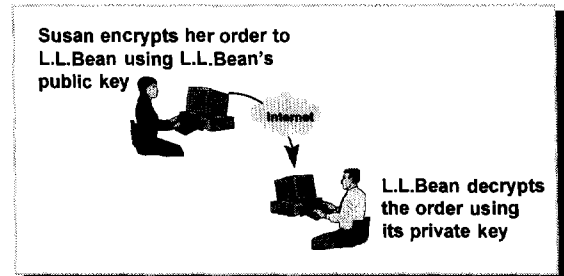


Figure 2. Example of public key application to place an order.

Digital Signatures. A digital signature is an electronic stamp or seal that can be appended to virtually any form of electronic transaction. Similar to a tamper-resistant seal on a package, a digital signature prevents someone from altering the data en route. Any attempt to change the data would be detected when the signature is verified.

A digital signature is created by generating a shortened version of the message, known as a hash. The sender then encrypts the hash with his or her private key.

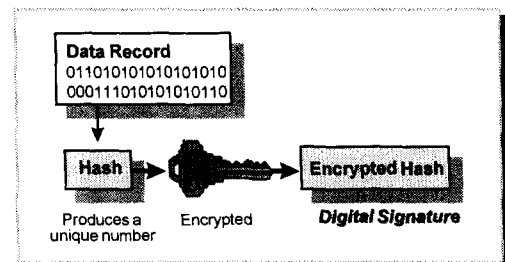


Figure 3. How a digital signature is calculated.

The sender appends the encrypted hash to the original data along with his or her public verification key, creating a digitally signed electronic message. Each digital signature is unique to the data hashed. If the data is altered in any way en route to its destination, the digital signature will fail validation by the receiver. Since the private key is used to encrypt the hash, a digital signature cannot be forged.

To verify the digital signature, the recipient recreates the hash using the message received and the same standard hashing algorithm. The encrypted hash of the original message is decrypted using the sender's public key and the two results are compared. If the two hash numbers match, the signature is validated.

Successfully decoding a hash with a particular public key provides a strong indicator that it was sent by the holder of the corresponding private key and that the message was not changed along the way. But how do we know the identity of the individual holding the key pair?

Digital Certificates. Before two parties exchange data using public key encryption, each wants to authenticate the identity of the other party. Consumers want to know that they are dealing with a real merchant – such as L.L. Bean or Lands' End – and not a spoofed site. Likewise, businesses want to know the true identity of the customer sending purchase information. One way to provide authentication is to rely on a trusted third party to issue and manage the distribution of digital certificates.

A digital certificate is a signed electronic document issued by a trusted third party, called a Certification Authority (CA), such as GTE CyberTrust™. Using circumstances and criteria defined by the customer, a CA manages the certificate process by issuing, renewing and revoking digital certificates for approved individuals.

To create a digital certificate, the CA creates a hash of the holder's identifying information and public key, encrypts the hash and appends it to the identifying information. If the identifying information or public key contained in the digital certificate is changed in any way, the certificate will fail validation.

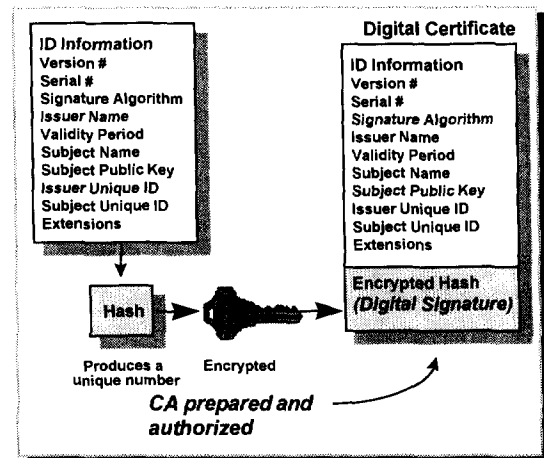


Figure 4. A certification authority is a trusted third party who vouches for the identity of a public key holder.

To check the validity of a digital certificate, the recipient recalculates the certificate hash using the same hashing algorithm on the certificate holder's identifying information and public key as it was received. Next, the original certificate hash is decrypted using the CA's public key. If the recalculated certificate hash is the same as the decrypted certificate hash, the certificate is valid.

Since a CA keeps its private key secret, its digital certificates provide an extremely reliable means of authentication. When used properly, providing that both the CA and the individual protect their private keys securely, digital signatures and digital certificates make it impossible for a hacker to impersonate another entity.

Glossary

Public Key Encryption – an encryption technique where the sender encodes a message using the recipient's public key that can only be decrypted by using the recipient's corresponding private key. Keys are characterized by their bit length and are created as public/private key pairs.

Hashing – a probabilistic unique shortened version of a message used as a "fingerprint" of the larger message. For example, one type of hash could be summing the ASCII values of all characters in a message.

Digital Signature – the encrypted hash of a message. If the message is changed in any way, the hash results also change showing that the message has been tampered with.

Digital Certificate – an electronic document that binds the identity of an individual or organization to a public key. Digital certificates are generated using identifying information (e.g., name, address, affiliation, etc.), a public key, a validity period and other management information. X.509 is the standard governing digital certificates.

Certification Authority (CA) – a trusted third party who generates digital certificates, thus vouching for the identity of the public key holder. The CA acts as a quasi-equivalent of an Internet Notary Public.

SET – Secure Electronic Transactions, a protocol for electronic commerce used for secure credit card transactions developed by MasterCard and Visa in conjunction with industry organizations including GTE, IBM, Microsoft, Netscape and Terisa.

Endnotes

¹Russ Maney, "Letter from the Director," *The Fourth Channel* (Forrester Research, Inc., September/October 1996), i.

²Vic Wheatman, quoted in "Year in Review," *c/net* (December 26, 1996). URL: <http://www.news.com>.

³Dick Peck, quoted in "Fewer Than One Percent of Sites Can Deliver Secure Transactions," *PC Week* (December 12, 1996). URL: <http://www.pcweek.com>.

⁴John Moreh, "In Digital Signatures We Trust," *Software Magazine* (January 1997): 115.

⁵David Stipp, "The Birth of Digital Commerce," *Fortune* (December 9, 1996): 159.

⁶Greg Tarmin, quoted in "To Charge or Not to Charge Online – That is the Question," *Yahoo! Internet Life* (October, 1996): 72.

⁷Michael Moeller and Jim Kerstetter, "Encryption Technology SET for Final Testing," *PC Week* (January 6, 1997): 1.

If you would like to learn more, please contact:



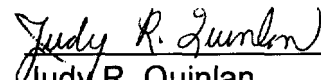
CyberTrust Sales and Marketing
77 A Street, Needham, MA 02194-2892 USA
Tel: 800-487-8788 Fax: 617-455-4003
E-mail: info@cybertrust.gte.com
URL: <http://www.cybertrust.gte.com>

ISO 9001 Registered

CyberTrust is a trademark of GTE Government Systems Corporation.
All other marks are the properties of their respective owners.

Certificate of Service

I, Judy R. Quinlan, hereby certify that copies of the foregoing "Reply Comments of GTE Service Corporation" have been mailed by first class United States mail, postage prepaid, on June 5, 1997 to all parties of record.



Judy R. Quinlan